AO 93 (Rev. 11/13) Search and Seizure Warrant

UNITED STATES DISTRICT COURT

for the

Eastern District of New York

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* (1) ONE TOSHIBA LAPTOP COMPUTER AND (2) ONE AT&T CELLULAR TELEPHONE	)	Case No. 20-M-282

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Eastern District of New York *(identify the person or describe the property to be searched and give its location)*:

See Attachment A

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See Attachment B

YOU ARE COMMANDED to execute this warrant on or before _____ *(not to exceed 14 days)*

☑ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to the Duty Magistrate Judge.

(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

☐ for _____ days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of _____.

Date and time issued: 04/01/2020 4:40 pm

Judge's signature

City and state: Brooklyn, New York

Hon. Ramon E. Reyes, Jr. U.S.M.J.

Printed name and title

Return

Case No.: 20-M-282	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

ATTACHMENT A

The property to be searched is (1) one Toshiba laptop computer Model Satellite P855-S5312, serial number 9C042258K; and (2) one AT&T cellular telephone Model Z223, serial number 322560052679, IMEI 868899020091605 (collectively, the "SUBJECT DEVICES").

This warrant authorizes the forensic examination of the SUBJECT DEVICES for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

Particular Things to be Seized

For the period from in or about November 2012 through in or about December 2017, all items, including records and information, that constitute evidence, fruits and instrumentalities relating to violations of 18 U.S.C. §§ 1343, 1344, 1349 (bank fraud, wire fraud and conspiracy to commit the same); 18 U.S.C. § 1028 (fraud in connection with identity documents and conspiracy to commit the same); 18 U.S.C. §§ 1028A and 371 (aggravated identity theft and conspiracy to commit the same); 18 U.S.C. § 1644 (fraudulent use of credit cards); and 18 U.S.C. §§ 1956, 1957 (money laundering and conspiracy to commit the same) (collectively, the "Subject Offenses"), including but not limited to:

a. Any and all records, including but not limited to, identifying documents, credit card & bank statements, applications to financial institutions, including banks and credit card companies, correspondence to/from financial institutions, bookkeeping records, including inventory records and accounting journals, records of wire and/or online transfers, deposit items, checks, withdrawal items, banking financial receipts, income tax returns, correspondences and applications to/from credit card/merchant processors, company bills, records identifying ownership of entities, emails, invoices, handwritten notes, and all account information, including login names, account passwords, security questions/answers, related to the following individuals and entities:

1. Moustafa Ayoub;
2. Claudia Ayoub;
3. Manife Ayoub;

4. Sobhi Ayoub;
5. Manife S. Ayoub;
6. Mohamed Ayoub;
7. Naim Ayoub;
8. Robert Elsaleh;
9. Constantine Vases;
10. Abed Ahmad;
11. Alaa Ahmad;
12. Freeform International, Inc.;
13. Blackstone Capital Group, LLC;
14. M&H Sportswear, Inc.;
15. Global Network Marketing Solutions, Inc.;
16. Swap Real Estate, LLC;
17. Silvermist, Inc.;
18. Everest, Inc.;
19. Clothing Zone;
20. Astoria Food Mart, Inc., a/k/a Cedar, a/k/a Al Nour
21. Milkway Knitwear, Inc.;
22. Melville Parkway, Inc.; and
23. Woodbury Port, Inc.

b. evidence of who used, owned or controlled the SUBJECT DEVICES, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

c. evidence of software that would allow others to control the SUBJECT DEVICES, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

d. evidence of the lack of such malicious software;

e. evidence indicating how and when the SUBJECT DEVICES were accessed or used to determine the chronological context of access, use, and events relating to crimes under investigation and to the SUBJECT DEVICES' user;

f. evidence indicating the SUBJECT DEVICES user's state of mind as it relates to the crimes under investigation;

g. evidence of the attachment to the SUBJECT DEVICES of other storage devices or similar containers for electronic evidence;

h. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the SUBJECT DEVICES;

i. evidence of the times the SUBJECT DEVICES were used;

j. passwords, encryption keys and other access devices that may be necessary to access the SUBJECT DEVICES;

k. documentation and manuals that may be necessary to access the SUBJECT DEVICES or to conduct a forensic examination of the SUBJECT DEVICES;

l. records of or information about Internet Protocol addresses used by the SUBJECT DEVICES;

m. records of or information about the SUBJECT DEVICES' Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and

n. contextual information necessary to understand the evidence described in this attachment.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

DMP:JGH/JEA
F. #2018R01373

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

IN THE MATTER OF THE SEARCH OF: (1) ONE TOSHIBA LAPTOP COMPUTER; AND (2) ONE AT&T CELLULAR TELEPHONE	APPLICATION FOR A SEARCH WARRANT FOR ELECTRONIC DEVICES Case No. 20-M-282

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, JOSEPH DORNBIERER, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—electronic devices—which are currently in the possession of law enforcement officers, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent with the Department of Homeland Security, Homeland Security Investigations ("HSI"). I have been a Special Agent with HSI for over 3 years, and a federal law enforcement officer for more than 15 years, during which I have been responsible for conducting and assisting investigations into, among other things, criminal

activity involving computers such as hacking, computer network intrusions, money laundering, check fraud, bank fraud, credit card fraud, and identity theft. I am currently assigned to HSI Cyber Division's Cyber Intrusion and Fraud Group. During my time with HSI, I have conducted or participated in surveillance, the execution of search warrants, debriefings of informants, and the review of other evidence. Through my training, education, and experience, I have become familiar with the manner in which people use computers to commit crimes and the law enforcement techniques that can be utilized to investigate and disrupt such activity. Moreover, in the course of my investigations and other cases on which I have worked, I have gained experience executing search warrants for both physical premises and electronic evidence and data, including the content and other data associated with cellphones, email, messenger, financial, and digital-marketplace accounts.

3. The property to be searched is (1) one Toshiba laptop computer Model Satellite P855-S5312, serial number 9C042258K (the "Toshiba laptop computer") and (2) one AT&T cellular telephone Model Z223, serial number 322560052679, IMEI 868899020091605 (the "AT&T cellular telephone") (collectively, the "SUBJECT DEVICES").

4. The applied-for warrant would authorize the forensic examination of the SUBJECT DEVICES for the purpose of identifying electronically stored data particularly described in Attachment B, which constitute evidence, fruits and instrumentalities of violations of, *inter alia*: 18 U.S.C. §§ 1343, 1344 and 1349 (bank fraud, wire fraud and conspiracy to commit the same); 18 U.S.C. § 1028 (fraud in connection with identity documents and conspiracy to commit the same); 18 U.S.C. §§ 1028A and 371 (aggravated identity theft and

conspiracy to commit the same); 18 U.S.C. § 1644 (fraudulent use of credit cards); and 18 U.S.C. §§ 1956 and 1957 (money laundering and conspiracy to commit the same) (collectively, the "Subject Offenses").

5. The source of your deponent's information and the grounds for his belief are as follows:[1]

6. The United States Attorney's Office for the Eastern District of New York, HSI, the Internal Revenue Service – Criminal Investigation ("IRS–CI"), the New York City Police Department and the New York County District Attorney's Office, are investigating a years-long conspiracy perpetrated by ABED AHMAD ("ABED"), ALAA AHMAD ("ALAA"), CLAUDIA AYOUB, MOUSTAFA AYOUB and CONSTANTINE VASES ("VASES"), and others. The investigation has revealed that from in or about November 2012 through in or about June 2017 (the "Charged Period"), these coconspirators conspired with each other and others to defraud JPMorgan Chase & Co. ("JPMC") and its customers by misappropriating more than $7.6 million from numerous victim bank accounts held at JPMC (the "JPMC Victim Accounts").

7. On February 3, 2020, this Court signed a Criminal Complaint (Mag. No. 20-106, hereinafter the "Complaint") and issued arrest warrants for ABED AHMAD, ALAA AHMAD, CLAUDIA AYOUB, MOUSTAFA AYOUB and CONSTANTINE VASES (collectively, "the Defendants") for conspiring together and with others to commit bank fraud

---

[1] Because the purpose of this affidavit is to set forth only those facts necessary to establish probable cause for a search warrant, I have not described all the relevant facts and circumstances of which I am aware.

and money laundering. The Complaint is attached hereto as Exhibit A and hereby incorporated by reference.

8. On March 18, 2020, a grand jury returned a three-count indictment (the "Indictment") charging Ayoub with (1) bank fraud conspiracy; (2) money laundering conspiracy; and (3) aggravated identity theft. See Crim. No. 20-142.

9. On March 24, 2020, the Honorable Ramon E. Reyes, Jr., United States Magistrate Judge for the Eastern District of New York, issued a search warrant under docket number 20-M-265 (the "March 24, 2020 Warrant"), authorizing the search of the premises known and described as the home office inside of 20-56 42nd Street, Queens, New York 11105 (the "SUBJECT PREMISES") and the Hewlett Packard Pavilion Desktop Computer (the "HP Desktop Computer") found therein. A copy of that search warrant is attached as Exhibit B to this affidavit and is incorporated by reference herein. A copy of the affidavit submitted in support of the application for that search warrant is attached as Exhibit C to this affidavit and is incorporated by reference herein.[2]

10. On March 25, 2020, HSI and other law enforcement agents executed the search warrant at the SUBJECT PREMISES. During the search, agents discovered, in addition to the HP Desktop Computer, the SUBJECT DEVICES in the SUBJECT PREMISES.

11. While I believe the search warrant affidavit submitted in support of the search warrant for the SUBJECT PREMISES issued by Judge Reyes on March 24, 2020

---

[2] The attached copy of the affidavit contains one redacted footnote. The unredacted copy, which was previously reviewed by this Court, is available in the file of the Clerk of the Court or upon request to the government.

already contains sufficient probable cause to search the SUBJECT DEVICES for evidence, fruits and instrumentalities of the Subject Offenses, in an abundance of caution I am seeking an additional warrant to do so and hereby providing the following additional information in support of this warrant.

12. Specifically, during the search of the SUBJECT PREMISES, law enforcement officers recovered the Toshiba laptop computer inside a laptop bag that contained evidence, fruits and instrumentalities of the Subject Offenses, including tax returns for Woodbury Port, Inc. ("Woodbury") and M&H Sportswear, Inc. ("M&H"). Additionally, next to the laptop bag law enforcement officers also recovered corporate records for Melville Parkway, Inc. ("Melville"), M&H and Woodbury.

13. As detailed in the Complaint, Woodbury was a shell company created using Manife Ayoub's name without her knowledge or consent while she was outside the United States. MOUSTAFA AYOUB and other coconspirators used Woodbury and financial accounts in its name to steal and transfer funds from JPMC Victim Accounts. Melville is a company created by CLAUDIA AYOUB which conducted no legitimate business and was used to open at least one bank account (the "Melville business bank account") that received money related to the bank fraud and money laundering conspiracies, including from checks deposited into this Melville business bank account in the names of associates of charged coconspirator CONSTANTINE VASES for no known legitimate purpose. Furthermore, records show payments made from the Melville business bank account to other coconspirators, including to CONTANTINE VASES and at least one sham business entity controlled by ABED AHMAD. Finally, as set forth in the Complaint, records show that M&H and its

associated financial accounts were used repeatedly by MOUSTAFA AYOUB and other coconspirators to receive, distribute and launder funds misappropriated from JPMC Victim Funds. Thus, there is probable cause to believe that the Toshiba laptop computer contains evidence, fruits and instrumentalities of the Subject Offenses.

14. The AT&T cellular telephone was found in a drawer next to the desk inside the SUBJECT PREMISES where the HP Desktop Computer was recovered. The desk also contained additional evidence, fruits and instrumentalities of the Subject Offenses, including multiple credit and/or bank cards in the name of CLAUDIA AYOUB, Manife Ayoub, M&H, Melville and Woodbury. Based on the investigation to date, I know that cellular phones were used by MOUSTAFA AYOUB and other coconspirators in furtherance of the charged bank fraud and money laundering conspiracies, including to make phone calls to financial institution impersonating individuals in furtherance of the conspiracies. Moreover, based on my knowledge, training and experience, I also know that individuals who commit the Subject Offenses, including aggravated identity theft, often use cellular phones in furtherance of such crimes.

15. In sum, there is probable cause to believe the SUBJECT DEVICES from the SUBJECT PREMISES contain evidence, fruits and instrumentalities of the Subject Offenses.

16. The SUBJECT DEVICES are currently in the lawful possession of HSI in the Eastern District of New York. In my training and experience, I know that the SUBJECT DEVICES have been stored in a manner in which their contents are, to the extent material to

this investigation, in substantially the same state as they were when the SUBJECT DEVICES first came into the possession of HSI.

TECHNICAL BACKGROUND

17. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a

variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System

(generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

f. Electronic Storage Media: Electronic storage media includes any physical object upon which electronic data can be recorded. Examples include USB drives, external hard drives, CDs, and DVDs.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

18. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed

via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

19. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the SUBJECT DEVICES were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence might be on the SUBJECT DEVICES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by

a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

20. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the SUBJECT DEVICES consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the SUBJECT DEVICES to human inspection in order to determine whether it is evidence described by the warrant.

21. *Manner of execution.* Because this warrant seeks only permission to examine SUBJECT DEVICES already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the SUBJECT DEVICES described in Attachment A to seek the items described in Attachment B.

Joseph Dornbierer

JOSEPH DORNBIERER
Special Agent
Department of Homeland Security, HSI

Sworn to before me this
1st day of April, 2020

THE HONORABLE RAMON E. REYES, JR.
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK

ATTACHMENT A

The property to be searched is (1) one Toshiba laptop computer Model Satellite P855-S5312, serial number 9C042258K; and (2) one AT&T cellular telephone Model Z223, serial number 322560052679, IMEI 868899020091605 (collectively, the "SUBJECT DEVICES").

This warrant authorizes the forensic examination of the SUBJECT DEVICES for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

Particular Things to be Seized

For the period from in or about November 2012 through in or about December 2017, all items, including records and information, that constitute evidence, fruits and instrumentalities relating to violations of 18 U.S.C. §§ 1343, 1344, 1349 (bank fraud, wire fraud and conspiracy to commit the same); 18 U.S.C. § 1028 (fraud in connection with identity documents and conspiracy to commit the same); 18 U.S.C. §§ 1028A and 371 (aggravated identity theft and conspiracy to commit the same); 18 U.S.C. § 1644 (fraudulent use of credit cards); and 18 U.S.C. §§ 1956, 1957 (money laundering and conspiracy to commit the same) (collectively, the "Subject Offenses"), including but not limited to:

a. Any and all records, including but not limited to, identifying documents, credit card & bank statements, applications to financial institutions, including banks and credit card companies, correspondence to/from financial institutions, bookkeeping records, including inventory records and accounting journals, records of wire and/or online transfers, deposit items, checks, withdrawal items, banking financial receipts, income tax returns, correspondences and applications to/from credit card/merchant processors, company bills, records identifying ownership of entities, emails, invoices, handwritten notes, and all account information, including login names, account passwords, security questions/answers, related to the following individuals and entities:

    1. Moustafa Ayoub;
    2. Claudia Ayoub;
    3. Manife Ayoub;

4. Sobhi Ayoub;
5. Manife S. Ayoub;
6. Mohamed Ayoub;
7. Naim Ayoub;
8. Robert Elsaleh;
9. Constantine Vases;
10. Abed Ahmad;
11. Alaa Ahmad;
12. Freeform International, Inc.;
13. Blackstone Capital Group, LLC;
14. M&H Sportswear, Inc.;
15. Global Network Marketing Solutions, Inc.;
16. Swap Real Estate, LLC;
17. Silvermist, Inc.;
18. Everest, Inc.;
19. Clothing Zone;
20. Astoria Food Mart, Inc., a/k/a Cedar, a/k/a Al Nour
21. Milkway Knitwear, Inc.;
22. Melville Parkway, Inc.; and
23. Woodbury Port, Inc.

b. evidence of who used, owned or controlled the SUBJECT DEVICES, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

c. evidence of software that would allow others to control the SUBJECT DEVICES, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

d. evidence of the lack of such malicious software;

e. evidence indicating how and when the SUBJECT DEVICES were accessed or used to determine the chronological context of access, use, and events relating to crimes under investigation and to the SUBJECT DEVICES' user;

f. evidence indicating the SUBJECT DEVICES user's state of mind as it relates to the crimes under investigation;

g. evidence of the attachment to the SUBJECT DEVICES of other storage devices or similar containers for electronic evidence;

h. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the SUBJECT DEVICES;

i. evidence of the times the SUBJECT DEVICES were used;

j. passwords, encryption keys and other access devices that may be necessary to access the SUBJECT DEVICES;

k. documentation and manuals that may be necessary to access the SUBJECT DEVICES or to conduct a forensic examination of the SUBJECT DEVICES;

l. records of or information about Internet Protocol addresses used by the SUBJECT DEVICES;

m. records of or information about the SUBJECT DEVICES' Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and

n. contextual information necessary to understand the evidence described in this attachment.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

EXHIBIT A

DMP:JGH/JEA/BFP
F. #2018R01373

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK
- X

UNITED STATES OF AMERICA

- against -

ABED AHMAD,
ALAA AHMAD,
CLAUDIA AYOUB,
MOUSTAFA AYOUB and
CONSTANTINE VASES,

Defendants.

TO BE FILED UNDER SEAL

COMPLAINT AND AFFIDAVIT IN SUPPORT OF APPLICATION FOR ARREST WARRANT

No. 20-MJ-106
(18 U.S.C. §§ 1349 and 1956(h))

- X

EASTERN DISTRICT OF NEW YORK, SS:

JEFFREY A. MILLER, being duly sworn, deposes and states that he is a Supervisory Special Agent with the Internal Revenue Service, duly appointed according to law and acting as such.

Bank Fraud Conspiracy

In or about and between November 2012 and June 2017, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendants ABED AHMAD, ALAA AHMAD, CLAUDIA AYOUB, MOUSTAFA AYOUB and CONSTANTINE VASES, together with others, did knowingly and intentionally conspire to execute and attempt to execute a scheme and artifice to defraud JPMorgan Chase & Co., a financial institution, and to obtain moneys, funds, credits, assets and other property under the custody and control of said financial institution, by means of one or more materially false and

fraudulent pretenses, representations and promises, contrary to Title 18, United States Code, Section 1344).

(Title 18, United States Code, Section 1349)

Money Laundering Conspiracy

In or about and between November 2012 and June 2017, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendants ABED AHMAD, ALAA AHMAD, CLAUDIA AYOUB, MOUSTAFA AYOUB and CONSTANTINE VASES, together with others, did knowingly and intentionally conspire to conduct one or more financial transactions in and affecting interstate commerce, which involved the proceeds of a specified unlawful activity, to wit; bank fraud conspiracy, knowing that the property involved in the financial transactions represented the proceeds of some form of unlawful activity and knowing that the transactions were designed in whole or in part to conceal and disguise the nature, the location, the source, the ownership and the control of the proceeds of the specified unlawful activity, contrary to Title 18, United States Code, Section 1956(a)(1)(B)(i).

(Title 18, United States Code, Section 1956(h))

The source of your deponent's information and the grounds for his belief are as follows:[1]

1. I have been employed as a Special Agent with the Internal Revenue Service–Criminal Investigation for approximately nineteen years. I am currently a

[1] Because the purpose of this Complaint is to set forth only those facts necessary to establish probable cause to arrest, I have not described all the relevant facts and circumstances of which I am aware.

Supervisory Special Agent assigned to the New York Field Office. I am responsible for, among other things, supervising, conducting and assisting in investigations into various white collar crimes including tax fraud, tax-related fraud, bank fraud, money laundering and identity theft. I have participated in and conducted numerous investigations, during the course of which I have interviewed suspects and witnesses, executed court-authorized search and arrest warrants, and used other investigative techniques to secure relevant information. As a result of my training and experience, I am familiar with techniques and methods of operation used by individuals involved in criminal activity to conceal their activities from detection by law enforcement.

2. I have personally participated in the investigation of the offenses discussed below. I am familiar with the facts and circumstances of this investigation from: (a) my supervision of and participation in this investigation; (b) my review of records and reports generated by other law enforcement agents in the United States and elsewhere, including interviews of witnesses; (c) my review of communications recovered during the investigation; and (d) information provided to me by other agents and law enforcement officials.

A. Overview

3. As set forth in detail herein, the investigation has revealed that from at least as early as November 2012 through at least June 2017 (the "Charged Period"), the defendants ABED AHMAD, ALAA AHMAD, CLAUDIA AYOUB, MOUSTAFA AYOUB and CONSTANTINE VASES (collectively, the "Defendants") conspired with each other and others, known and unknown, to defraud JPMorgan Chase & Co. ("JPMC") and its customers by stealing millions of dollars from more than forty individual JPMC bank accounts, many of

which were held by bank branches in Queens, New York. The Defendants also conspired with each other and others to launder the proceeds of their fraud by, among other things, using a complex web of financial transactions, shell entities, business and personal financial accounts and fictitious and stolen identities to receive, hide and ultimately transfer stolen funds to themselves and other coconspirators. In total, the Defendants and their coconspirators engaged in more than 900 financial transactions to misappropriate more than $7.6 million of JPMC victim funds (the "JPMC Victim Funds") through each of their fraudulent means, which they then laundered and distributed among themselves and other coconspirators.

B. The Defendants

ABED AHMAD & ALAA AHMAD

4. From approximately September 2007 to May 2014, ABED AHMAD ("ABED") worked as a manager at a JPMC branch located in Astoria, Queens. From at least November 2012 until he left JPMC in approximately May 2014, ABED abused his position of trust at the bank by repeatedly using its internal computer systems to access the customer account profiles of bank accounts belonging to more than 60 individual JPMC bank customers. ABED had no known legitimate business purpose for accessing these accounts, most of which were held by customers who were deceased by the time ABED began accessing their accounts. ABED accessed high-dollar value accounts, many of which were primarily funded by recurring benefit payments from the United States Social Security Administration and Department of Veterans Affairs.

5. ALAA AHMAD ("ALAA"), ABED's brother, worked for JPMC from approximately December 2008 until January 2017, most recently as a relationship banker at a Queens branch. While working at JPMC, ALAA also repeatedly used the internal computer

systems to access high-value accounts, also with no known legitimate business purpose for doing so.

6. In total, ABED and ALAA accessed more than 80 JPMC accounts held in the names of approximately 64 individual bank customers (the "JPMC Victim Accounts"), all of which were subsequently drained of the majority of their funds as part of the bank fraud and money laundering conspiracies described herein.

7. ABED and ALAA left their employment with JPMC before their criminal activity was discovered. ABED and ALAA both received a share of the misappropriated funds from the JPMC Victim Accounts for their roles in the bank fraud and money laundering conspiracies. After leaving JPMC, ABED and ALAA relocated to Florida and began operating Nai Restaurant, LLC ("Nai"), which did business as a restaurant under the name La Vie Lebanese Restaurant ("La Vie"). As set forth in greater detail below, records show that ABED's and ALAA's coconspirators, including MOUSTAFA AYOUB and CONSTANTINE VASES, funded a significant portion of the cost of La Vie using money stolen from the JPMC Victim Accounts that were improperly accessed by ABED and ALAA.

MOUSTAFA AYOUB & CLAUDIA AYOUB

8. The investigation has revealed that in furtherance of the bank fraud and money laundering conspiracies charged herein, MOUSTAFA AYOUB ("MOUSTAFA"), along with his other coconspirators, including his girlfriend CLAUDIA AYOUB ("CLAUDIA"), created and controlled numerous bank and credit card accounts, as well as businesses and shell entities, using the names and identifying information of multiple individuals, including family members and other associates, to create a web of financial transactions to disguise the nature, source, location, ownership and origin of the money that

MOUSTAFA, CLAUDIA and the other coconspirators misappropriated from the JPMC Victim Accounts.

9. Both MOUSTAFA and CLAUDIA reside in Queens, New York and lived there throughout the Charged Period. From approximately 2011 to 2015, MOUSTAFA and CLAUDIA rented an apartment on 29th Street in Astoria, Queens (the "29th Street Address"). MOUSTAFA, CLAUDIA and other coconspirators repeatedly used the 29th Street Address to create and manage a string of financial accounts and business entities that they used to transfer, launder and distribute among themselves misappropriated JPMC Victim Funds.

10. Additionally, in approximately 2012, MOUSTAFA and CLAUDIA purchased a home on 42nd Street in Astoria, Queens (the "42nd Street Address"). MOUSTAFA and CLAUDIA also used this address to operate numerous financial accounts used to misappropriate and launder JPMC Victim Funds.

11. The investigation has revealed that MOUSTAFA and CLAUDIA received more than $2 million in misappropriated JPMC Victim Funds during the Charged Period. They did so by, among other things, using numerous financial accounts and business entities, including shell companies, tied to their 29th Street Address and 42nd Street Address.

CONSTANTINE VASES

12. CONSTANTINE VASES ("VASES") is tax preparer and self-identified accountant who resides in Long Island, New York and works in Queens, New York. VASES helped manage shell companies, including Freeform International, Inc. and Blackstone Capital Group, LLC, which were used to receive and redistribute stolen JPMC Victim Funds among VASES and his coconspirators. VASES also produced fraudulent financial documentation,

including fictitious bank statements and invoices for goods and services and at least one fraudulent tax return, all in furtherance of the bank fraud and money laundering conspiracies. Furthermore, records, including a review of VASES's emails obtained pursuant to a judicially authorized search warrant, show that VASES was the purported accountant for entities controlled by ABED and MOUSTAFA that were used to launder JPMC Victim Funds during the Charged Period.

13. VASES received at least approximately $600,000 in JPMC Victim Funds during the Charged Period, including a significant portion laundered through multiple accounts before ultimately being transferred into VASES's home equity line of credit (the "VASES HELOC Account") against his home in Queens, New York, which VASES and his wife owned from approximately 2016 through March 2019.

C. The Assumed Identities

14. The investigation has also revealed that the Defendants repeatedly used the names and personally identifiable information ("PII") of numerous people, including the holders of JPMC Victim Accounts. In particular, the Defendants used the identities of real individuals to create and operate more than 40 financial accounts central to the bank fraud and money laundering conspiracies. One such individual ("Individual-1") lived in Brooklyn until July 2011. Records show that on or about July 29, 2011, Individual-1 left the United States and has not returned since. A second such individual ("Individual-2"), lived in Queens until on or about September 4, 2014 when he/she left the United States. Individual-2 has not returned to the United States.

15. Records, including bank and credit card statements, show that after Individual-1 and Individual-2 left the United States, MOUSTAFA, CLAUDIA, VASES and

other members of the conspiracy used their names and PII, including their dates of birth and driver's license information, to operate numerous bank and credit card accounts and business entities to misappropriate and launder JPMC Victim Funds. In total, the Defendants and their coconspirators used such bank and credit card accounts to transfer approximately $6 million from JPMC Victim Accounts directly into accounts in the names of Individual-1 and Individual-2, which were controlled by the Defendants and their coconspirators.

16. By way of illustration, MOUSTAFA and CLAUDIA operated numerous bank and credit card accounts in Individual-1's name that were directly tied to the 29th Street Address and 42nd Street Address. These accounts received and laundered money stolen from JPMC Victim Accounts. For example, records show that a Citibank Account in Individual-1's name ending 9814 (the "Individual-1 9814 Account") was registered to the 29th Street Address, years after Individual-1 left the United States. The Individual-1 9814 Account received approximately $1.1 million in JPMC Victim Funds, much of which was subsequently transferred to personal and business bank accounts controlled by MOUSTAFA, CLAUDIA, VASES and other coconspirators. Records further show that the Individual-1 9814 Account was also used on at least one occasion in 2014 to pay the monthly rent for the 29th Street Address. The payment was made via a check drawn on the Individual-1 9814 Account and purportedly signed by Individual-1 despite his/her having been outside the United States since approximately September 2011. Furthermore, bank security records show MOUSTAFA and CLAUDIA in March and April 2017 depositing laundered JPMC Victim Funds into the Individual-1 9184 account.

17. As another example, a Citibank account in Individual 2's name and ending 1797 (the "Individual-2 1797 Account") was registered to a P.O. Box in Astoria, New

York. Bank records show that the Individual-2 1797 Account was used on multiple occasions to launder and distribute JPMC Victim Funds among the coconspirators, including to pay tens of thousands of dollars of JPMC Victim Funds to the VASES HELOC Account.

D. The Business Entities Used to Receive and Launder Misappropriated Funds

18. In addition to using assumed identities to perpetrate the bank fraud and money laundering conspiracies, the Defendants and their coconspirators also used a series of business entities to receive, transfer, launder and distribute proceeds from the fraud, including multiple shell entities whose sole purpose was to facilitate the frauds. In fact, by establishing many of these shell companies, members of the conspiracy, including ABED, ALAA, MOUSTAFA, CLAUDIA and VASES, were able to control bank accounts, acquire credit cards and obtain point-of-sale credit card terminals ("POS terminals") [2] used to misappropriate and launder JPMC victim funds.

Nai Restaurant, LLC & La Vie

19. Records show that on or about March 4, 2016, Nai restaurant was registered using the address of a residence owned by ALAA in Florida. ABED lived at this residence from approximately 2015 to 2018, and ALAA lived there with him from approximately 2017 to 2018. Records show also that ABED and another relative are managers of Nai which, as set forth above, did business as La Vie. Records show that MOUSTAFA, CLAUDIA and VASES funded a significant portion of the cost of La Vie using misappropriated JPMC Victim Funds.

---

[2] A POS terminal is an electronic device used to process card payments at retail locations. A POS terminal generally does the following: reads the information off a customer's credit or debit card and checks whether the funds in a customer's bank account are sufficient.

Swap Real Estate & Global Network Marketing Solutions

20. During the Charged Period, ABED registered Swap Real Estate, LLC ("Swap") in Florida and Global Network Marketing Solutions Incorporated ("Global") in New York. Records show that both businesses existed in name only and were used as pass-through entities for ABED, ALAA and their coconspirators to launder and distribute misappropriated JPMC Victim Funds. During the Charged Period, both ABED and ALAA used financial accounts in the name of Global and Swap to receive stolen JPMC Victim Funds.

M&H Sportswear, Inc.

21. M&H Sportswear, Inc. ("M&H") is a purported sportswear company based in Queens, New York, and doing business under the name "Clothing Zone, Inc." Records show that MOUSTAFA is M&H's CEO and that the business address is the 29th Street Address. In addition to its corporate filings, numerous bank accounts and other records link M&H to the 29th Street Address and the 42nd Street Address. Records further show that M&H and its associated financial accounts were used repeatedly by MOUSTAFA, CLAUDIA, VASES and other coconspirators to receive, distribute and launder JPMC Victim Funds.

Astoria Food Mart, Inc.

22. Records show that during the Charged Period, MOUSTAFA was also the president and owner of a Queens restaurant and grocery store, known at various points in time as Astoria Food Mart, Inc. ("Astoria Food"), Nour Foods and Cedars Meat House. This business, one of the only brick-and-mortar locations used in furtherance of the charged conspiracies, was used by MOUSTAFA, CLAUDIA and others to receive and launder JPMC Victim Funds, including laundered payments of such funds to Global, the shell entity controlled by ABED and ALAA. For example, between approximately February and April

2014, five payments totaling approximately $88,000 of laundered JPMC Victim Funds were paid via check to Global from Astoria Food bank accounts controlled by MOUSTAFA.

Woodbury Port, Inc.

23. Woodbury Port, Inc. ("Woodbury") was registered in New York on or about November 18, 2014. Woodbury's address was registered as the 42nd Street Address. Records show that Woodbury is a shell company which, in fact, does no real business. In financial account documents for Woodbury, MOUSTAFA's daughter is listed as the president. Records show that at the time Woodbury was registered in New York, MOUSTAFA's daughter was living outside of the United States. After Woodbury was registered, approximately three bank and credit card accounts were opened in its name at various financial institutions, with MOUSTAFA's daughter as the sole signatory. One of these accounts, also registered to the 42nd Street Address, was used to receive JPMC Victim Funds and to distribute those funds to ABED, ALAA, MOUSTAFA, CLAUDIA and VASES, among others.

24. For example, records, including bank security footage, show that from approximately September through November 2016, ALAA deposited more than $80,000 of JPMC Victim Funds into a Swap business bank account for which ABED was a signatory. The deposits were made in multiple transactions via checks drawn on a Woodbury bank account for which MOUSTAFA's daughter was the sole signatory and which was registered using the 42nd Street Address. The primary source of the funds transferred from Woodbury to Swap from the checks deposited by ALAA came from JPMC Victim Accounts accessed by ABED and ALAA.

25. Furthermore, records, including bank security footage, also show that on or about October 10, 2016, ALAA deposited into a bank account in his name a check for

approximately $5,000 drawn on the same Swap account into which he deposited more than $80,000 as described above.

Freeform International, Inc.

26. On or about February 19, 2013, Freeform International, Inc. ("Freeform") was registered in New York. Records show that the company's address is the 29th Street Address. Freeform holds itself out as a wholesale apparel company; in fact, it does no real business. Instead, VASES, MOUSTAFA, and other coconspirators opened numerous bank and credit card accounts in Freeform's name throughout the Charged Period that were used to receive and distribute JPMC Victim Funds.

27. For example, on or about November 24, 2014, two Freeform business accounts were opened online at Wells Fargo. These Freeform accounts, ending -8025 (the "WF-8025 Account") and -8033 (the "WF-8033 Account") each listed Freeform's address as the 29th Street Address. Individual-1 was the sole signatory on both these business accounts, despite Individual-1's absence from the United States since July 2011. These Freeform accounts received and laundered JPMC Victim Funds, which were then distributed to ABED, CLAUDIA, MOUSTAFA, VASES and other coconspirators. For example, records show that at least one check written from the WF-8025 Account and purportedly signed by Individual-1 was used to pay CLAUDIA and MOUSTAFA's rent at the 29th Street Address. Additionally, bank security records from February and March 2017 show CLAUDIA cashing multiple checks drawn from the WF-8025 Account payable to Woodbury.

28. As another example, approximately $700,000 of laundered JPMC Victim Funds were paid from a Freeform Bank of America bank account to an M&H bank

account controlled by MOUSTAFA and CLAUDIA. Individual-1 was again listed as the sole signatory on the Freeform account, which was registered to the 29th Street Address in 2014.

29. In total, the Defendants used Freeform and its associated financial accounts to misappropriate more than $2 million of JPMC Victim Funds.

Blackstone Capital Group, LLC

30. Records show that Blackstone Capital Group, LLC ("Blackstone") was incorporated as an LLC in New York on or about March 1, 2010 and registered to the accounting firm where VASES works in Astoria, Queens. In Blackstone's 2012 New York State biennial filing, VASES signed the filing and identified himself as a "Member" of the company. As with Freeform, the investigation has revealed that VASES and other members of the conspiracy used bank and credit card accounts in the name of Blackstone to receive and launder stolen JPMC Victim Funds.

31. Specifically, records show that VASES worked to obtain POS terminals and merchant account services for both Freeform and Blackstone. The terminals, which were delivered to VASES's office, were then used to charge nearly $2 million worth of fictitious sales paid with JPMC Victim Funds.

E. Bank Account Transfers

32. The Defendants conspired with each other and others to misappropriate JPMC Victim Funds in two central ways. The first method was to transfer money directly from the JPMC Victim Accounts accessed by ABED and ALAA while they were working at JPMC. These initial transfers were made predominantly through fraudulent checks, online and wire transfers into numerous "First Pass" bank accounts held at various financial

institutions.[3] The majority of these First Pass financial accounts were held in the names of Individual-1 and Individual-2, and controlled and operated by the Defendants and their coconspirators. The Defendants and their coconspirators then used these First Pass accounts to transfer the stolen funds and launder them through a second layer of personal and business bank accounts used and controlled by the Defendants and other members of the conspiracy, including into the accounts of shell companies they created and controlled. The Defendants and their coconspirators then further laundered the stolen funds by transferring them to other financial accounts that they controlled.

33. By way of illustration, on or about November 13, 2012, ABED used JPMC's internal computer system to access the bank account information of a JPMC customer ("Victim-1"). At the time ABED began accessing Victim-1's account (the "Victim-1 Account"), Victim-1 had been deceased for approximately ten years and the account had a balance of approximately $650,000. Victim-1 was the sole signatory on the Victim-1 Account and, with the exception of automatic deposits and regularly scheduled debit transactions, the account had been dormant for years. ABED had no known legitimate business purpose for accessing the Victim-1 Account.

34. On or about November 16, 2012, four days after ABED first accessed the Victim-1 Account within JPMC's computer systems, a JPMC online account was created for the Victim-1 Account.

---

[3] First Pass refers to the initial transfer of JPMC Victim Funds from the JPMC Victim Accounts into a set of financial accounts controlled and managed by members of the conspiracy.

35. Records show that between approximately November 13, 2012 and July 23, 2013, ABED used JPMC's internal computer systems to access the Victim-1 Account at least 20 more times, all for no known legitimate business purpose. During the same period, approximately $500,000 was misappropriated and transferred out of the Victim-1 Account. The transfers were made primarily through fraudulent checks purportedly signed by Victim-1, as well as by a wire transfer.

36. The majority of funds transferred from the Victim-1 Account were transferred to a First Pass account held in the name of Individual-1. The account, which was controlled by the Defendants and other members of the conspiracy, was held at JPMC and ended in 9119 ("the "Indvidual-1 9119 Account"). Records show that approximately eight transactions were executed drawing off a total of approximately $500,000 from the Victim-1 Account. Three of these transactions were checks purportedly signed by Victim-1, despite his/her being deceased for ten years, and deposited into the Individual-1 9119 Account. Those transactions, totaling more than $275,000 in Victim-1 funds, were as follows:

- Check # 468 dated January 28, 2013 payable to Individual-1 for $95,500 with the memo line "Mortgage Down Payment" deposited into the Indvidual-1 9119 Account at JPMC and posted on February 1, 2013.

- Check # 474 dated January 30, 2013 payable to Individual-1 for $94,512.65 with the memo line "Estate Account" deposited into the Indvidual-1 9119 Account at JPMC and posted on January 30, 2013.

- Check # 482 dated February 4, 2013 payable to Individual-1 for $86,129.60 with the memo line "Final Payment MTG L045-39624685S" deposited into the Indvidual-1 9119 Account at JPMC and posted on February 4, 2013.

37. Almost immediately after the misappropriated Victim-1 Account funds were deposited into the Individual-1 9119 Account, approximately $86,500 was laundered and

distributed to accounts held by MOUSTAFA and VASES. Specifically, on or about January 31, 2013, $75,000 was transferred from the Individual-1 9119 Account into the VASES HELOC Account. Then, on or about February 1, 2013, approximately $11,500 was transferred to MOUSTAFA's business account for M&H.

38. Furthermore, bank records show that, through the use of three other First Pass accounts, the Defendants transferred and laundered an additional $225,000 from the Victim-1 Account into accounts controlled by MOUSTAFA, CLAUDIA and VASES, including to the VASES HELOC Account and additional bank accounts in the name of M&H and Astoria Food controlled by MOUSTAFA.

39. Records show that ABED also used his position at JPMC to access the Individual-1 9119 Account within JPMC's internal computer systems on multiple occasions around the time of the above-described transactions, again for no known legitimate business purpose.

40. By July 2013, ABED and his coconspirators had misappropriated hundreds of thousands of dollars from the Victim-1 Account. At around this time, ABED submitted to JPMC a power of attorney request purporting to be from Victim-1 giving permission to Individual-1 to control the remaining funds in the Victim-1 Account. When JPMC risk management personnel followed-up with ABED on this power of attorney request, ABED falsely stated that he had spoken to Victim-1 and that Victim-1 had personally approved the power of attorney as well as checks previously written from the Victim-1 Account to Individual-1 for, among other things, a mortgage payment. In fact, at the time, Victim-1 had been deceased for approximately ten years. Ultimately, JPMC denied the power of attorney request. Furthremore, at around the time in July 2013 that ABED provided false information

to JPMC, he also used JPMC's internal computer systems to again access the Victim-1 Account multiple times for no known legitimate purpose.

41. The investigation has revealed that, in a likely effort to avoid such scrutiny in the future, the Defendants stopped using paper checks to misappropriate JPMC Victim Funds and instead began using online and wire transfers to do so. For example, records show that on or about November 9, 2013, ABED used his position at JPMC to access the account of another JPMC customer ("Victim-2") approximately three times for no known legitimate business purpose. At the time, Victim-2 had resided outside the United States for years and his/her account (the "Victim-2 Account") had been dormant for years, other than regularly-scheduled interest payments to the account. Victim-2 was the sole signatory on the account.

42. When ABED first accessed the Victim-2 Account on or about November 9, 2013, it had a balance of approximately $1 million. Shortly thereafter, beginning on or about November 14, 2013, and continuing through on or about December 19, 2013, approximately eight transfers were executed from the Victim-2 Account to a First Pass account controlled by the Defendants. Specifically, eight wire transfers totaling approximately $1 million were made from the Victim-2 Account to a TD Ameritrade Account ending 9144 held in the name of Individual-1 (the "Individual-1 9144 Account"). Immediately before the first transfer of funds received from the Victim-2 Account, the Individual-1 9144 Account had a negative account balance.

43. Records show that the Individual-1 9144 Account was created on or about November 17, 2011, approximately three months after Individual-1 left the United States. Both the P.O. Box and email account used to open Individual-1 9144 Account are

linked to numerous other financial accounts opened in Individual-1's name and which were used to launder JPMC Victim Funds, including payments to MOUSTAFA and CLAUDIA.

44. Records further show that once the misappropriated funds from the Victim-2 Account reached the Individual-1 9144 Account, the coconspirators further laundered the proceeds by transferring approximately $1 million in misappropriated funds into two different accounts held in the name of Individual-1: a Bank of America account (the "Individual-1 5833 Account") and the Individual-1 9814 Account, which is described above. The money was laundered to these two accounts using approximately fifteen wire transfers executed from approximately November 18, 2013 through January 22, 2014.

45. The Defendants then further laundered the funds from the Victim-2 Account and distributed the proceeds among themselves. Specifically, between December 2013 and February 2014, MOUSTAFA received more than $100,000 in Victim-2 funds via checks purportedly signed by Victim-2 made payable to MOUSTAFA's business, Astoria Food, and deposited into MOUSTAFA-controlled bank accounts. MOUSTAFA then paid tens of thousands of dollars of these funds to ABED through transfers to Global, ABED's shell entity. Additionally, as set forth above, records, including bank security camera records, show that CLAUDIA and MOUSTAFA used the Individual-1 9814 Account to make deposits of JPMC Victim Funds.

46. The investigation has revealed that during the Charged Period, the Defendants used the above-described scheme to misappropriate and launder more than $4 million in JPMC Victim Funds from numerous JPMC Victim Accounts, all of which were accessed by ABED or ALAA using JPMC's internal computer systems.

F. Credit Card Transfers

47. The other primary method the Defendants used to misappropriate JPMC Victim Funds involved transferring the funds from JPMC Victim Accounts to make payments to a series of credit card accounts controlled and operated by the Defendants and their coconspirators. The Defendants used credit cards in the names of Individual-1 and Individual-2 to charge sales by the shell companies they controlled, like Freeform and Blackstone, principally using the POS terminals obtained by VASES. They then transferred funds from the JPMC Victim Accounts to pay these charges, which had the effect of transferring the JPMC Victim Funds to the shell companies controlled by the Defendants. The Defendants also transferred personal credit card balances to the credit cards in the names of Individual-1 and Individual-2, and then used JPMC Victim Funds to pay off the credit card balances.

48. Specifically, approximately 24 credit card accounts in Individual-1's and Individual-2's names received approximately $2 million in payments directly from JPMC Victim Accounts. Approximately $1.2 million more was paid to business credit card accounts for which Individual-1 and Individual-2 were the signatories.

49. For example, between approximately 2015 and 2017, an American Express ("Amex") credit card ending 23-1004 in the name of Blackstone and Individual-2 (the "Individual-2 Amex Account") received more than $700,000 in payments from approximately 16 JPMC Victim Accounts. Records, including Internet Protocol ("IP") data, show that this Amex account was opened in the United States after Individual-2 left the country. The account charged more than $700,000 in fictitious sales at Freeform, the shell company controlled by MOUSTAFA and VASES. Records further show that a Freeform bank account

funded in part by the fictitious sales subsequently transferred misappropriated JPMC Victim Funds to VASES, MOUSTAFA and other coconspirators and entities controlled by them, including Woodbury.

50. As another example, between approximately 2015 and 2016, an American Express credit card in Individual-1's name ending 35-1005 (the "Individual-1 Amex Account") received approximately $2,500 in payments from a JPMC Victim Account accessed by ALAA using JPMC's computer systems. Records, including IP data, show that the Individual-1 Amex Account was opened in the United States after Individual-1 left the country and that the address for the account was the 29th Street Address. Records further show that in August 2016, MOUSTAFA used the Individual-1 Amex Account to purchase eyeglasses.

51. Records also show that a credit card opened at First National Bank of Omaha in Individual-2's name after he/she left the United States received payments of more than $50,000 during the Charged Period from approximately three JPMC Victim Accounts accessed by ABED and ALAA. Records show that on or about December 22, 2014, ABED attempted to use the First National Bank credit card account to make a purchase at Costco.

52. As another example, a TD Bank credit card in Individual-1's name received approximately $39,000 in funds misappropriated from a JPMC Victim Account. Records show that on or about March 17, 2016, CLAUDIA used the credit card to make a purchase at a CVS store near her residence in Astoria, Queens.

53. In total, ABED, ALAA, CLAUDIA, MOUSTAFA and VASES conspired together and with others to misappropriate approximately $3.2 million using the credit-card scheme described above. Of this $3.2 million, approximately $1.7 million of

misappropriated JPMC Victim Funds was transacted through Freeform and distributed through multiple financial transactions to accounts maintained and controlled by the coconspirators.

WHEREFORE, your deponent respectfully requests that arrest warrants issue for defendants ABED AHMAD, ALAA AHMAD, CLAUDIA AYOUB, MOUSTAFA AYOUB and CONSTANTINE VASES, so that they may be dealt with according to law. I further request that this affidavit, and the arrest warrants, be filed under seal as premature disclosure of this application would give the Defendants an opportunity to destroy evidence, harm or threaten victims or other witnesses, change patterns of behavior, notify confederates and flee or evade prosecution, with the exception that the complaint and arrest warrants are unsealed for the limited purpose of disclosing the existence of or disseminating the complaint and/or arrest warrant to relevant U.S., foreign or intergovernmental authorities, at the discretion of the United States and in connection with efforts to prosecute the defendants or secure the defendants' arrest, extradition or expulsion, or as otherwise required for the purposes of national security.

S/ Jeffrey Miller
JEFFREY A. MILLER
Supv. Special Agent, Internal Revenue Service

Sworn to before me this
3rd day of February, 2020

S/ Roanne Mann
THE HONORABLE ROANNE L. MANN
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK

EXHIBIT B

AO 93 (Rev. 11/13) Search and Seizure Warrant

UNITED STATES DISTRICT COURT

for the

Eastern District of New York

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* THE PREMISES KNOWN AND DESCRIBED AS THE HOME OFFICE INSIDE OF 20-56 42ND STREET, QUEENS, NEW YORK 11105, AND THE HEWLETT PACKARD PAVILION DESKTOP COMPUTER FOUND THEREIN	)	Case No. 20-M-265

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Eastern District of New York *(identify the person or describe the property to be searched and give its location)*:

See Attachment A

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See Attachment B

YOU ARE COMMANDED to execute this warrant on or before April 7, 2020 *(not to exceed 14 days)*

☑ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to the Duty Magistrate Judge.
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

☐ for _____ days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of _____.

Date and time issued: 03/24/2020 4:12 am

Judge's signature

City and state: Brooklyn, New York

Hon. Ramon E. Reyes, Jr. U.S.M.J.
Printed name and title

AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2)

Return

Case No.: 20-M-265	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

ATTACHMENT A

Property to be Searched

The property to be searched is the first floor home office inside of the private residence located at 20-56 42nd Street in Queens, New York 11105 (the "SUBJECT PREMISES"), to include the Hewlett Packard Pavilion desktop computer. Upon entering the side door entrance of the 20-56 42nd Street residence, the SUBJECT PREMISES to be searched is located to the left on the first floor of the house.

ATTACHMENT B

Property to be Seized

1. For the period from in or about November 2012 through in or about December 2017, all items, including records and information, that constitute evidence, fruits and instrumentalities relating to violations of 18 U.S.C. §§ 1343, 1344, 1349 (bank fraud, wire fraud and conspiracy to commit the same); 18 U.S.C. § 1028 (fraud in connection with identity documents and conspiracy to commit the same); 18 U.S.C. §§ 1028A and 371 (aggravated identity theft and conspiracy to commit the same); 18 U.S.C. § 1644 (fraudulent use of credit cards); and 18 U.S.C. §§ 1956, 1957 (money laundering and conspiracy to commit the same) (collectively, the "Subject Offenses"), including but not limited to:

(a) Any and all records, including but not limited to, identifying documents, credit card & bank statements, applications to financial institutions, including banks and credit card companies, correspondence to/from financial institutions, bookkeeping records, including inventory records and accounting journals, records of wire and/or online transfers, deposit items, checks, withdrawal items, banking financial receipts, income tax returns, correspondences and applications to/from credit card/merchant processors, company bills, records identifying ownership of entities, emails, invoices, handwritten notes, and all account information, including login names, account passwords, security questions/answers, related to the following individuals and entities:

1. Moustafa Ayoub;
2. Claudia Ayoub;
3. Manife Ayoub;
4. Sobhi Ayoub;
5. Manife S. Ayoub;
6. Mohamed Ayoub;
7. Naim Ayoub;
8. Robert Elsaleh;
9. Constantine Vases;
10. Abed Ahmad;
11. Alaa Ahmad;
12. Freeform International, Inc.;
13. Blackstone Capital Group, LLC;
14. M&H Sportswear, Inc.;
15. Global Network Marketing Solutions, Inc.;
16. Swap Real Estate, LLC;
17. Silvermist, Inc.;
18. Everest, Inc.;
19. Clothing Zone;
20. Astoria Food Mart, Inc., a/k/a Cedar, a/k/a Al Nour
21. Milkway Knitwear, Inc.;

22. Melville Parkway, Inc.; and
23. Woodbury Port, Inc.

(b) Any and all credit cards, debit cards, bank cards and store membership cards;

(c) All documents, including bills, related to cell phones held in the names of Moustafa Ayoub and Naim Ayoub;

(d) Point of sale terminals;

(e) Computers or storage media used as a means to commit the Subject Offenses, including the Hewlett Packard Pavilion desktop computer;

(f) For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

i. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

ii. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

iii. evidence of the lack of such malicious software;

iv. evidence indicating how and when the COMPUTER was accessed or used to determine the chronological context of COMPUTER access, use, and events relating to crime under investigation and to the COMPUTER user;

v. evidence indicating the COMPUTER user's state of mind as it relates to the crime under investigation;

vi. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

vii. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

viii. evidence of the times the COMPUTER was used;

ix. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

x. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

xi. records of or information about Internet Protocol addresses used by the COMPUTER;

xii. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

xiii. contextual information necessary to understand the evidence described in this attachment.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

EXHIBIT C

DMP:JGH/JEA
F. #2018R01373

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

IN THE MATTER OF AN APPLICATION OF THE UNITED STATES OF AMERICA FOR A SEARCH WARRANT FOR THE PREMISES KNOWN AND DESCRIBED AS THE HOME OFFICE INSIDE OF 20-56 42ND STREET, QUEENS, NEW YORK 11105, AND THE HEWLETT PACKARD PAVILION DESKTOP COMPUTER FOUND THEREIN	APPLICATION FOR A SEARCH WARRANT 20-M-265

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, JOSEPH DORNBIERER, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as the home office inside of 20-56 42nd Street, Queens, New York 11105 (the "SUBJECT PREMISES"), and the Hewlett Packard Pavilion desktop computer found therein, as further described in Attachment A, for the things described in Attachment B.

2. I am a Special Agent with the Department of Homeland Security, Homeland Security Investigations ("HSI"). I have been a Special Agent with HSI for over 3 years, and a federal law enforcement officer for more than 15 years, during which I have been responsible for conducting and assisting investigations into, among other things, criminal

activity involving computers such as hacking, computer network intrusions, money laundering, check fraud, bank fraud, credit card fraud, and identity theft. I am currently assigned to HSI Cyber Division's Cyber Intrusion and Fraud Group. During my time with HSI, I have conducted or participated in surveillance, the execution of search warrants, debriefings of informants, and the review of other evidence. Through my training, education, and experience, I have become familiar with the manner in which people use computers to commit crimes and the law enforcement techniques that can be utilized to investigate and disrupt such activity. Moreover, in the course of my investigations and other cases on which I have worked, I have gained experience executing search warrants for both physical premises and electronic evidence and data, including the content and other data associated with cellphones, email, messenger, financial, and digital-marketplace accounts.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on the facts set forth in this Affidavit, I respectfully submit that there is probable cause to believe that there presently is located in the SUBJECT PREMISES certain items and property, which are more fully set forth in Attachment B, which constitute evidence, fruits and instrumentalities of violations of, *inter alia*: 18 U.S.C. §§ 1343, 1344 and 1349 (bank fraud, wire fraud and conspiracy to commit the same); 18 U.S.C. § 1028 (fraud in connection with identity documents and conspiracy to commit the same); 18 U.S.C. §§ 1028A and 371 (aggravated identity theft and conspiracy to commit the same); 18 U.S.C. § 1644 (fraudulent use of credit cards); and 18 U.S.C. §§ 1956 and 1957 (money laundering and conspiracy to commit the same) (collectively, the "Subject Offenses").

DESCRIPTION OF SUBJECT PREMISES

5. The SUBJECT PREMISES to be searched is the first floor home office inside of the private house located at 20-56 42nd Street, Queens, New York 11105 (the "42nd Street Residence"), and to include the Hewlett Packard Pavilion desktop computer (the "HP Desktop Computer"). Upon entering the side door entrance of the 20-56 42nd Street residence, the SUBJECT PREMISES to be searched is located to the left on the first floor of the house.

PROBABLE CAUSE

I. Background

6. The United States Attorney's Office for the Eastern District of New York, HSI, the Internal Revenue Service – Criminal Investigation ("IRS–CI"), the New York City Police Department and the New York County District Attorney's Office, are investigating a years-long conspiracy perpetrated by ABED AHMAD ("ABED"), ALAA AHMAD ("ALAA"), CLAUDIA AYOUB, MOUSTAFA AYOUB and CONSTANTINE VASES ("VASES"), and others. The investigation has revealed that from in or about November 2012 through in or about June 2017 (the "Charged Period"), these coconspirators conspired with each other and others to defraud JPMorgan Chase & Co. ("JPMC") and its customers by misappropriating more than $7.6 million from numerous victim bank accounts held at JPMC (the "JPMC Victim Accounts").

7. On February 3, 2020, this Court signed a Criminal Complaint (Mag. No. 20-106, hereinafter the "Complaint") and issued arrest warrants for ABED, ALAA, CLAUDIA AYOUB, MOUSTAFA AYOUB and VASES (collectively, "the Defendants") for conspiring

together and with others to commit bank fraud and money laundering. The Complaint is attached hereto as Exhibit 1 and hereby incorporated by reference.

8. On February 4, 2020, the Defendants were arrested and charged pursuant to the Complaint. Both MOUSTAFA AYOUB and CLAUDIA AYOUB[1] were arrested at the SUBJECT PREMISES address. On March 18, 2020, a grand jury in the Eastern District of New York returned a three-count indictment (the "Indictment") charging MOUSTAFA AYOUB with one count of bank fraud conspiracy, one count of money laundering conspiracy and one count of aggravated identity theft. See Crim. No. 20-142 (ENV). The Indictment includes a forfeiture allegation against the 42nd Street Residence based upon the property's use in facilitating the charged money laundering offense. The United States is continuing to investigate the involvement of additional coconspirators in the Subject Offenses, as well as multiple additional acts of, *inter alia*, aggravated identity theft and fraudulent use of credit cards committed by MOUSTAFA AYOUB and others.

9. As detailed in the Complaint, the Defendants conspired with each other and others to misappropriate funds from the JPMC Victim Accounts in two central ways. The first method was to transfer money directly from the JPMC Victim Accounts that were accessed by ABED and ALAA while they were working at JPMC. These initial transfers were made predominantly through fraudulent checks, online and wire transfers into numerous "First Pass" bank accounts held at various financial institutions.[2] The majority of these First

---

[1] The Complaint indicated Claudia Ayoub is Moustafa Ayoub's girlfriend. The investigation has since revealed that Claudia and Moustafa Ayoub were married in Mexico approximately ten years ago, though the marriage may not be legally valid.

[2] "First Pass" refers to the initial transfer of funds from the JPMC Victim

Pass financial accounts were held in the names of (1) Naim Ayoub, who is referred to in the Complaint as Individual-1 and who left the United States in approximately July 2011 and has not returned since, and (2) Robert Elsaleh, who is referred to in the Complaint as Individual-2 and who left the United States in approximately September 2014 and has not returned since. In reality, however, and as set forth in detail in the Complaint, these First Pass financial accounts were controlled and operated by the Defendants and their coconspirators. The Defendants and their coconspirators then used these First Pass accounts to transfer the stolen funds and launder them through a second layer of personal and business bank accounts used and controlled by the Defendants and other members of the conspiracy, including into the accounts of shell companies they created and controlled. The Defendants and their coconspirators then further laundered the stolen funds by transferring them to other financial accounts that they controlled. Using this method, the Defendants misappropriated and laundered millions of dollars from JPMC Victim Accounts.

10. The other primary method the Defendants used to misappropriate funds from the JPMC Victim Accounts involved transferring the funds from JPMC Victim Accounts to make payments to a series of credit card accounts controlled and operated by the Defendants and their coconspirators. The Defendants used credit cards, again in the names of Naim Ayoub and Robert Elsaleh, to charge sales by the shell companies they controlled, principally using point of sale ("POS") terminals obtained by VASES. They then transferred funds from the JPMC Victim Accounts to pay these charges, which had the effect of transferring the funds

---

Accounts into a set of financial accounts controlled and managed by members of the conspiracy.

from the JPMC Victim Accounts to the shell companies controlled by the Defendants. The Defendants also transferred personal credit card balances to the credit cards in the names of Naim Ayoub and Robert Elsaleh, and then used funds from the JPMC Victim Accounts to pay off the credit card balances.

11. The investigation, including a review of bank and credit card records, has revealed that the following entities and/or financial accounts held in their names, were used in furtherance of the bank fraud and money laundering conspiracies charged in the Complaint, as well as fraud in connection with identity documents and credit card fraud: Freeform International, Inc.; Blackstone Capital Group, LLC; M&H Sportswear, Inc.; Clothing Zone; Global Network Marketing Solutions, Inc.; Swap Real Estate, LLC; Silvermist, Inc.; Everest, Inc.; Astoria Food Mart, Inc., a/k/a Cedar, a/k/a Al Nour; Milkway Knitwear, Inc.; Melville Parkway, Inc.; and Woodbury Port, Inc.

II. MOUSTAFA AYOUB and the SUBJECT PREMISES

12. The SUBJECT PREMISES is located inside the 42nd Street Residence, the current residence of MOUSTAFA AYOUB,[3] CLAUDIA AYOUB and their children. As set forth in the Complaint, the 42nd Street Residence containing the SUBJECT PREMISES was used by MOUSTAFA AYOUB and CLAUDIA AYOUB in furtherance of the bank fraud and money laundering conspiracies to, among other things, operate numerous bank and credit card accounts used to receive and/or launder funds stolen from JPMC Victim Accounts.

[3] MOUSTAFA AYOUB is currently detained at the Metropolitan Detention Center in Brooklyn pending trial on the charges contained in the Indictment.

13. For example, the investigation has revealed that MOUSTAFA AYOUB used the 42nd Street Residence as the address for multiple financial accounts that he opened and operated in the name of his adult daughter, Manife Ayoub.[4] Indeed, records and other evidence show that MOUSTAFA AYOUB repeatedly used Manife Ayoub's name and personally identifiable information ("PII"), including her social security number, to open and operate these financial accounts while Manife Ayoub was living outside the United States, all without her knowledge or consent. MOUSTAFA AYOUB operated these accounts in Manife Ayoub's name, including multiple bank accounts, in furtherance of the conspiracies charged in the Indictment.

14. Several of the bank accounts that MOUSTAFA AYOUB unlawfully opened in Manife Ayoub's name using the 42nd Street Residence address were used to receive and/or launder hundreds of thousands of dollars of stolen JPMC victim funds. For example, records show that in or about January 2015, while Manife Ayoub was living outside the United States, MOUSTAFA AYOUB used the internet to apply for and open a checking account at Citibank in the name of Manife Ayoub ending in the numbers 0285 (the "Manife Ayoub 0285 Account"). The online application for the Manife Ayoub 0285 Account shows that MOUSTAFA AYOUB used Manife Ayoub's social security number and date of birth to open the account, and that he listed the 42nd Street Residence as the account address. The investigation has revealed that the Manife Ayoub 0285 Account was used by MOUSTAFA AYOUB to receive tens of thousands of dollars of unlawfully misappropriated funds from JPMC Victim Accounts as part of the bank fraud conspiracy charged in the Indictment.

---

[4] Manife Ayoub is identified as "Jane Doe #1" in Count Three of the Indictment.

15. Furthermore, bank records, including phone calls recorded by the financial institutions as part of their regular course of business, show that on multiple occasions during the Charged Period, MOUSTAFA AYOUB used the telephone number 718-606-1518 to call the companies pretending to be Manife Ayoub. During these calls, MOUSTAFA AYOUB used Manife Ayoub's PII to operate one or more credit card accounts that MOUSTAFA AYOUB opened in her name without her knowledge or consent.

16. Records further show that 718-606-1518 is a telephone registered to the 42nd Street Residence in the name of "Claudia Ayoub." The email account associated with the telephone number is "clothingzone@aol.com," an email address used and controlled by MOUSTAFA AYOUB.

17. Additionally, a review of bank and Internet Protocol ("IP") records shows that the IP address associated with the 42nd Street Residence was registered in the name of CLAUDIA AYOUB and was used to log in to multiple financial accounts in the name of, among others, Manife Ayoub, in furtherance of the Subject Offenses. For example, IP records show that from approximately May through December 2016, the IP address associated with the SUBJECT PREMISES address was used numerous times to log in to a Capital One business credit card account in the name of Manife Ayoub ending in 5539 (the "Manife Ayoub Capital One 5539 Account"). The Manife Ayoub Capital One 5539 Account was opened in Manife Ayoub's name without her knowledge or consent in or about December 2015, when Manife Ayoub was living outside the United States, using the 42nd Street Residence as the account address. The business associated with the Manife Ayoub Capital One 5539 Account is listed as Woodbury Port, Inc. As detailed in the Complaint, Woodbury Port, Inc. was a shell company created using Manife Ayoub's name without her knowledge or consent while

she was outside the United States. MOUSTAFA AYOUB and other coconspirators used Woodbury Port and bank accounts in its name to steal funds from JPMC Victim Accounts.

18. Furthermore, as set forth above, both MOUSTAFA AYOUB and CLAUDIA AYOUB were arrested on February 4, 2020 at the 42nd Street Residence. While conducting a security sweep inside the 42nd Street Residence, including the SUBJECT PREMISES, a law enforcement officer observed, in plain view atop the desk inside the SUBJECT PREMISES, two stacks of what appeared to be credit and/or bank cards, with each stack appearing to contain approximately twenty to twenty-five cards.

19. The government has also received information from a confidential source ("CS-1")[5] that the SUBJECT PREMISES contains evidence of the Subject Offenses. Specifically, CS-1 has informed law enforcement that the HP Pavilion Computer located atop

5 [redacted]

the desk inside the SUBJECT PREMISES is a computer that MOUSTAFA AYOUB has used for approximately the last 5 years. CS-1 has further informed law enforcement that the computer contains a copy of Manife Ayoub's social security number, as well as a copy of Manife Ayoub's New York State identification card.

20. CS-1 has further informed law enforcement that atop the desk inside the SUBJECT PREMISES is a pad of paper containing the handwritten account passwords and security questions for numerous financial accounts in the name of multiple individuals, including CS-1. CS-1, who is familiar with MOUSTAFA AYOUB's handwriting, has informed law enforcement that the handwriting on the pad is MOUSTAFA AYOUB's handwriting. CS-1 has also informed law enforcement that the desk inside the SUBJECT PREMISES contains a folder with documents in the names of MOUSTAFA AYOUB's parents. Bank records show that in or about May 2014, two financial accounts – one at E-Trade and one at TD Ameritrade – were opened in the name of MOUSTAFA AYOUB's father, Sobhi Ayoub. Bank records further show that the address associated with these two accounts was MOUSTAFA AYOUB's and CLAUDIA AYOUB's rental apartment on 29th Street in Queens, New York, which, as set forth in the Complaint, MOUSTAFA AYOUB continued to pay rent for after he and CLAUDIA AYOUB moved to the 42nd Street Residence. Also as set forth in the Complaint, the 29th Street residence, just like the 42nd Street Residence, was used as an address for numerous fraudulently operated financial accounts used to commit the charged bank fraud and money laundering conspiracies.

21. Bank records also show that in or about April 2014, a TD Ameritrade account was opened in the name of MOUSTAFA AYOUB's mother, Manife S. Ayoub, and that the address associated with the account was the 29th Street residence.

22. At the time these three accounts were opened in the names of MOUSTAFA AYOUB's parents, they were living outside of the United States.

23. Based on my training and experience – including my participation in this investigation – I have learned that individuals who engage in fraudulent conduct such as the Subject Offenses as described herein often keep physical evidence, fruits, and instrumentalities of their crimes inside their home offices and stored and saved within computers inside those home offices.

24. Additionally, I know from my knowledge, training and experience that such evidence, fruits and instrumentalities are often stored in locked containers, safes, secret compartments, closets, drawers, above or below ceiling and floor tiles, behind false walls and, when digital in nature, inside locked or lockable electronic devices (e.g., computers and smart telephones) and in other places intended to avoid detection by other people, including law enforcement.

25. Accordingly, and based on all of the above, I submit that there is probable cause to believe that the SUBJECT PREMISES, including the HP Pavilion Computer found therein, will contain evidence, fruits and instrumentalities of the Subject Offenses.

TECHNICAL TERMS

26. Based on my training and experience, I use the following technical terms to convey the following meanings:

(a) IP Address: The Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so

that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

(b) Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

(c) Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

COMPUTERS, ELECTRONIC STORAGE AND FORENSIC ANALYSIS

27. As described above and in Attachment B, this application seeks permission to search for certain documents and records that might be found inside the SUBJECT PREMISES, including on the HP Pavilion Computer therein, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

28. *Probable cause.* I submit that if a computer or storage medium is found on the SUBJECT PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

(a) Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

(b) Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

(c) Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

(d) Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

29. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the SUBJECT PREMISES, including the HP Pavilion Computer, because:

(a) Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

(b) As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional

information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information

within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

(c) A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

(d) The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

(e) Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

30. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media, such as the HP Pavilion Computer, often requires the seizure of the physical storage

media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

(a) The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

(b) Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the SUBJECT PREMISES. However, taking the storage media off-

site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

(c) Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

31. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the law enforcement officers executing this warrant to image, or otherwise copy, storage media that reasonably appear to contain some or all of the evidence described in the warrant, including the HP Pavilion Computer, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant. In the event that the law enforcement officers executing the warrant are unable to image, or otherwise copy, storage media encompassed by the warrant on-site, the warrant I am applying for would permit law enforcement officers executing the warrant to seize such storage media for a reasonable amount of time, in order to complete the imaging, or other copying, process at an off-site location.

32. Because several people share the SUBJECT PREMISES, it is possible that the SUBJECT PREMISES will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that that it is possible that the things described in this warrant could be found on any of those

computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

CONCLUSION

WHEREFORE, your deponent respectfully requests that a warrant be issued, pursuant to Federal Rule of Criminal Procedure 41, to search the SUBJECT PREMISES, which is the first floor home office inside the 42nd Street Residence, as further described in Attachment A, and to seize those items set forth in Attachment B, including the HP Pavilion Computer, that may constitute evidence, fruits and instrumentalities of violations of the Subject Offenses.

JOSEPH DORNBIERER
Special Agent, HSI

Sworn to before me this
24th day of March, 2020

THE HONORABLE RAMON E. REYES, JR.
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK

ATTACHMENT A

Property to be Searched

The property to be searched is the first floor home office inside of the private residence located at 20-56 42nd Street in Queens, New York 11105 (the "SUBJECT PREMISES"), to include the Hewlett Packard Pavilion desktop computer. Upon entering the side door entrance of the 20-56 42nd Street residence, the SUBJECT PREMISES to be searched is located to the left on the first floor of the house.

ATTACHMENT B

Property to be Seized

1. For the period from in or about November 2012 through in or about December 2017, all items, including records and information, that constitute evidence, fruits and instrumentalities relating to violations of 18 U.S.C. §§ 1343, 1344, 1349 (bank fraud, wire fraud and conspiracy to commit the same); 18 U.S.C. § 1028 (fraud in connection with identity documents and conspiracy to commit the same); 18 U.S.C. §§ 1028A and 371 (aggravated identity theft and conspiracy to commit the same); 18 U.S.C. § 1644 (fraudulent use of credit cards); and 18 U.S.C. §§ 1956, 1957 (money laundering and conspiracy to commit the same) (collectively, the "Subject Offenses"), including but not limited to:

(a) Any and all records, including but not limited to, identifying documents, credit card & bank statements, applications to financial institutions, including banks and credit card companies, correspondence to/from financial institutions, bookkeeping records, including inventory records and accounting journals, records of wire and/or online transfers, deposit items, checks, withdrawal items, banking financial receipts, income tax returns, correspondences and applications to/from credit card/merchant processors, company bills, records identifying ownership of entities, emails, invoices, handwritten notes, and all account information, including login names, account passwords, security questions/answers, related to the following individuals and entities:

1. Moustafa Ayoub;
2. Claudia Ayoub;
3. Manife Ayoub;
4. Sobhi Ayoub;
5. Manife S. Ayoub;
6. Mohamed Ayoub;
7. Naim Ayoub;
8. Robert Elsaleh;
9. Constantine Vases;
10. Abed Ahmad;
11. Alaa Ahmad;
12. Freeform International, Inc.;
13. Blackstone Capital Group, LLC;
14. M&H Sportswear, Inc.;
15. Global Network Marketing Solutions, Inc.;
16. Swap Real Estate, LLC;
17. Silvermist, Inc.;
18. Everest, Inc.;
19. Clothing Zone;
20. Astoria Food Mart, Inc., a/k/a Cedar, a/k/a Al Nour
21. Milkway Knitwear, Inc.;

22. Melville Parkway, Inc.; and
23. Woodbury Port, Inc.

(b) Any and all credit cards, debit cards, bank cards and store membership cards;

(c) All documents, including bills, related to cell phones held in the names of Moustafa Ayoub and Naim Ayoub;

(d) Point of sale terminals;

(e) Computers or storage media used as a means to commit the Subject Offenses, including the Hewlett Packard Pavilion desktop computer;

(f) For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

i. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

ii. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

iii. evidence of the lack of such malicious software;

iv. evidence indicating how and when the COMPUTER was accessed or used to determine the chronological context of COMPUTER access, use, and events relating to crime under investigation and to the COMPUTER user;

v. evidence indicating the COMPUTER user's state of mind as it relates to the crime under investigation;

vi. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

vii. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

viii. evidence of the times the COMPUTER was used;

ix. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

x. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

xi. records of or information about Internet Protocol addresses used by the COMPUTER;

xii. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

xiii. contextual information necessary to understand the evidence described in this attachment.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.